

Risk Advisory Services

Auditorías de Seguridad

Auditorías de Seguridad

ANTECEDENTES

El CSI/FBI realizó una evaluación a 500 corporaciones y agencias de gobierno y detectó que el 90% afirmó tener intrusiones en su red y el 80% reconocieron pérdidas económicas (el 40% cuantificaron su pérdida financiera en 455,848,000 dólares, y el 40% detectó que la penetración se llevó a cabo desde afuera).

Según cifras de Gartner Group, de 300 *sites* auditados, el 97% son vulnerables a ataques. Asimismo, se descubrió que el 70% de los ataques ocurren a nivel de la aplicación web.

El informe *Amenazas a la Seguridad en Internet* publicado por la empresa de seguridad informática Symantec revela que el actual entorno de amenazas se caracteriza por un aumento en el robo y fuga de datos, así como la creación de códigos maliciosos dirigidos con el fin de robar información confidencial que puede ser utilizada con fines económicos.

EL MUNDO	"Los ciberataques a grandes compañías van en aumento en todo el mundo".
EXPANSIÓN	"Un ataque informático infecta 74.000 ordenadores en 196 países"
CINCO DÍAS	"La Seguridad Social sufre un nuevo ataque de phishing"

AUDITORÍA DE SEGURIDAD

Su empresa será capaz de protegerse contra los incidentes de seguridad que puedan producirse en los Sistemas de Información.



ALCANCE

Nuestras auditorías de seguridad comprenden el análisis, verificación y propuestas de mejora en los siguientes aspectos:

AUDITORÍA DE SEGURIDAD INTERNA

Enfocado a los servicios de red interna, servidores internos y equipos de usuario

Su objetivo es evaluar la seguridad de los sistemas frente a un posible ataque interno. Se ejecutan desde sus instalaciones pruebas en modo "Caja Blanca" o "Caja Negra":

- Sondeos de red y obtención de información.
- Detección de posibles fugas de información a través de la Red Pública.
- Escaneo de puertos e identificación de sistemas operativos.
- Análisis automatizados y manual de vulnerabilidades.
- Análisis de fortaleza de contraseñas de usuario.

AUDITORÍA DE SEGURIDAD DE RED

Enfocado a todos los equipos de Red

Su objetivo es evaluar la seguridad de los equipos de red ante un posible ataque interno. Se ejecutan desde sus instalaciones:

- Sondeos de red y obtención de información.
- Escaneo de puertos e identificación de servicios.
- Análisis automatizados y manual de vulnerabilidades.
- Análisis de estructura de red, segmentación y políticas de filtrado.
- Análisis de configuración de los equipos de red.
- Análisis y auditoría de red inalámbrica (WIFI).
- Análisis de Sistemas de detección y prevención de intrusos.

AUDITORÍA DE SEGURIDAD DE APLICACIÓN

Enfocado a todas las Aplicaciones de desarrollo del negocio

Su objetivo es evaluar la seguridad de las aplicaciones frente a un posible ataque interno:

- Análisis funcional de la Aplicación.
- Sondeos de red y obtención de información.
- Detección de posibles fugas de información a través de la Red Pública.
- Escaneo de puertos e identificación de sistemas operativos.
- Análisis automatizados y manual de vulnerabilidades.
- Validación de entradas de datos desde el usuario y manipulación de parámetros.
- Análisis de gestión de sesiones y métodos de autenticación.
- Detección de *Buffer Overflows*.

AUDITORÍA DE SEGURIDAD FÍSICA E INGENIERÍA SOCIAL

Enfocado a los Sistemas de seguridad física y empleados de la Organización

Su objetivo es evaluar los mecanismos de seguridad física y concienciación de usuarios en materia de seguridad:

- Análisis de la Seguridad del edificio y de su perímetro.
- Comprobación de los desechos de oficina – *Dumpster Diving*.
- Identificación de sensibilización de los usuarios en materia de seguridad.
- Test de intrusión físico.
- Test de ingeniería social. Envío de correos tipo *phishing*, llamadas telefónicas.

TEST DE INTRUSIÓN / PENTEST

Enfocado a todas las Aplicaciones de desarrollo del negocio

Su objetivo es evaluar la seguridad de los sistemas frente a un posible ataque externo. Se ejecuta desde las instalaciones de BDO efectuando:

- Sondeos de red y obtención de información.
- Detección de posibles fugas de información a través de la Red Pública.
- Escaneo de puertos, identificación de servicios y sistemas operativos.
- Análisis automatizado de vulnerabilidades.
- Análisis manual de vulnerabilidades.
- Test no privilegiado de aplicaciones externas.
- Test de medidas de contención frente a la llegada de código malicioso.
- Test de antivirus y ataque de ingeniería social.

METODOLOGÍAS Y ESTÁNDARES UTILIZADOS



International
Organization for
Standardization



PARA MÁS INFORMACIÓN:

GONZALO GARCÍA-LIÑÁN

Socio | Risk Advisory Services
gonzalo.garcia-linan@bdo.es

Esta publicación ha sido redactada en términos generales y debe ser contemplada únicamente como una referencia general. Esta publicación no puede utilizarse como base para amparar situaciones específicas y usted no debe actuar, o abstenerse de actuar, de conformidad con la información contenida en este documento sin obtener asesoramiento profesional específico. Póngase en contacto con BDO en cualquiera de nuestras oficinas para tratar estos asuntos en el marco de sus circunstancias particulares. BDO, sus socios y empleados, no aceptan ni asumen cualquier responsabilidad ante cualquier pérdida derivada de cualquier acción realizada o no por cualquier individuo al amparo de la información contenida en esta publicación o ante cualquier decisión basada en ella.

BDO Auditores, S.L.P. es una sociedad limitada española independiente y miembro de la red internacional de BDO, constituida por empresas independientes asociadas de todo el mundo, y creada por BDO International Limited, una compañía limitada por garantía del Reino Unido.

BDO es la marca comercial utilizada por toda la red BDO y para todas sus firmas miembro.

Copyright © 2026. Todos los derechos reservados. Publicado en España.

bdo.es
bdo.global